M-1

8 NOV 1977

OS 7 8072

MEMORANDUM FOR: Chairman, DCID 1/16 Revision Working Group
Intelligence Community Staff

FROM: [redacted] STAT
Chief, Information Security Group

SUBJECT: DCID 1/16

1. The attached memorandum for the record represents the preliminary findings of the Agency's Interdirectorate Task Force on DCID 1/16. Full coordination within the Agency continues as interested components review the issues of concern.

2. We are aware of the timeliness involved with the coordination process and are attempting to expedite this review within the Agency. Any questions regarding the attached may be directed to [redacted] (secure). STAT

[redacted] STAT

Attachment

30 October 1987

MEMORANDUM FOR THE RECORD

SUBJECT: DCID 1/16 Task Force

1. Introduction: The purpose of this memorandum for the record is to document the findings of the Agency's Interdirectorate Task Force on Director of Central Intelligence Directive (DCID) 1/16.

2. Background: DCID 1/16 is DCI policy for the protection of classified intelligence processed in Automated Information Systems (AIS) and networks. There has been no change to the policy since it was originally promulgated in 1979, although it was reissued in 1983 with only cosmetic changes. The current policy is badly outdated in terms of technology and security understanding. The Intelligence Community (IC) Staff took action to rewrite DCID 1/16 in order to address the critical issues of todays information systems. The Agency established an Interdirectorate Task Force to identify issues of concern, propose additions and/or changes, and develop a position on DCID 1/16 as drafted by the IC Staff. The task force met on 21 August and 28 September 1987. Those representing the directorates were: [redacted], DS&T: [redacted] DI: [redacted]

25X1 25X1 25X1

[redacted]

3. Issues: The following issues were identified and respective positions established by the task force:

Issue I: The DCID Confuses Policy and Implementation. The general consensus of task force members concerning the draft was that it blends implementation with policy.

Position 1: This blending causes confusion which will introduce implementation risks. Members of the task force felt the need to separate the implementation requirements from the policy. The policy should then be clearly stated to avoid ambiguity.

agree it mixes policy + procedures JUST AS OLD DCID/ MANUAL + MOST OTHER DCIDs DO, No change

25X1

[redacted]

~~CONFIDENTIAL~~

Issue II: The Accreditation Process. The DCID presents a formal life cycle accreditation process consisting of a system of requirements definition, certification, reporting, recordkeeping, and review and evaluation. The National Foreign Intelligence Board (NFIB) members are each designated as Principal Accrediting Authorities (PAA). AIS or networks operating in the compartmented mode may only be accredited by the NFIB members.

The DCID states that the authority to accredit compartmented systems cannot be further delegated.

Disagree in principal. See new last sentence of 3b of DCID

✓

Position 2: Unanimously, the representatives of the directorates agreed that delegation of authority is needed. The delegation would allow the deputy directors of each directorate to accredit their own dedicated, system high, and compartmented mode systems. This would be against a standard established by the NFIB member which is consistent with the minimum requirements of the DCID.

The DCID has no point of interaction for data owners to state protection requirements.

[redacted]

25X1

Position 3: Task Force members recommended that the data owner have an input to the accreditation process. The data owner should have a responsibility to specify the level of trust for processing the information. [See para 19, p. 24 of manual]

DCID says ~~that~~ owner can identify add'l requirement

The DCID requires periodic reaccreditation on all AIS every three years and on networks every five years.

✓

Position 4: In conjunction with position two, the task force agreed that whereas the authority to accredit an AIS or network should not be further delegated, the deputy directors should be able to delegate the reaccreditation authority.

Do Not agree; see new last sentence of 3b of DCID

The DCID does not make a strong enough statement that accreditation is an assumption of risk.

what's wrong with para 3a of DCID? See item (9)

Position 5: The discussion of accreditation needs to ensure that managers realize "trusted systems" still have an associated risk and that the accreditor is assuming that risk.

agree that "trusted" systems involve risk, but do not understand wh

where CIA wants this further explained.

NSA = emphasize "trusted products"
CIA = emphasize trusted "systems"

Issue III: Requirements for Use of NCSC Trusted Products. The DCID states that "all organizations processing intelligence... must acquire trusted products when feasible." The goal is to replace existing system component inventory with trusted products by CY 2000.

Position 6: Task Force members unanimously objected to the wording "must acquire trusted products." The document refers to the NCSC's EPL and trusted products as the Community-wide standard. The PAA has the authority to accredit its systems and must be able to decide what entities are trusted. DCID 1/16 should identify the security requirements; it should not dictate how individual agencies accomplish those requirements. The wording should reflect that agencies "must acquire trusted systems" and that the goal should be to have trusted systems by CY 2000 employing certified products. The PAA must have the flexibility to certify products which are not on the EPL. The task force felt that the EPL should be a mechanism to help in the certification process rather than a set of standards for certified products.

note that "when feasible" is deleted fm DCID wording

directly contradicts NSA comments

paras 5

See NSA changes.

up front "assumption of risk"

Issue IV: Minimum Security Requirements for AIS. Under Section III concerns were raised regarding the Interim Approval to Operate, Automated Guard Processors and Security Filters, and Protection of Storage Devices.

The DCID states that the interim approval to operate "shall not exceed one year in length."

Position 7: Phased system development is required for implementation of the complex systems being built today. Many of these will take 5 to 10 years. The ability to provide interim approvals beyond one year is necessary in order to accomplish phased implementation.

Disagree; NSA + DIA did not object. Accrediting Authorities can allow beyond 1 yr by granting an exception.

In regard to Automated Guard Processes(ors) and Security Filters, the DCID states: "For example, if, in the absence of an automated Guard, a system were operating in the multilevel mode, the system must be accredited for multilevel operation. The automated guard must meet the minimum security requirements for a system operating at the multilevel mode."

See change

Position 8: Members felt that adding ", and" between the two sentences would clarify the later statement as part of the example and not a specific requirement. Our position is that Guards can be used as permanent elements used to implement a trusted system. ✓

agree; see change to para 27

Regarding the protection of High Density/Transportable Storage devices, the DCID states that "the containers of all media shall be marked with the highest classification level and handling procedures of the information <u>ever</u> stored on the media..."

para 33

Position 9: Members felt the word "ever" should be changed "~~to~~ which can be." The requirement should call for all media to be marked prior to use with the level of data that it will be used to process. Relabeling media each time a tape is changed/used would present an unwarranted administrative burden and would be an error prone process. ✓

O.K. with some mods

Regarding the marking of printed output the draft states that individual pages of output must be marked as appropriate to reflect classification, and that a "manual review process is required for Dedicated and System High modes."

para 34 35 36 37 Double check ref NSA comments

Position 10: This requirement would prove to be an enormous burden given the volume of Agency processing. A clause should be included to the effect that "where markings cannot be trusted, a manual review is required." A manual review should only be required when the output is disseminated beyond the security control of the AIS facility. ✓

O.K. See revised wording in para 37

4. This represents the issues of concern and the proposed additions and/or changes to DCID 1/16 as identified by the Agency task force.

[redacted] 25X1

cc: C/ISG/OS/DA
ISO/DS&T
DBSB/ISD/OIR/DI [redacted] 25X1
C/IMS/ISS/DO
OSD/EG/OIT/DA [redacted] 25X1
C/PMB/PSG/CSD-OC/DA